TITLE: FEDERATED LEARNING: A FALSE SENSE OF SECURITY?

My T. Thai, Ph.D.
UF Research Foundation Professor
mythai@cise.ufl.edu

Monday, August 28, 9:55 am Central Time

Virtual Zoom Meeting:
https://zoom.us/j/9762699678?pwd=RUp5ZmN3cHUyQ1FvUExVQjVsc1hVUT09
Meeting ID: 976 269 9678
Passcode: K91Bwy

LECTURE ABSTRACT

Abstract: Federated Learning (FL) has emerged as a promising large-scale collaborative learning framework for its potential to protect user privacy and security. However, this promise has been constantly challenged. In this talk, we show that FL in its primitive form offers little to no privacy and security protection, by analyzing several attack vectors, both from malicious users to a dishonest server. Even with a layer of protection from differential privacy and secure aggregation, we further demonstrate that current FL implementation provides no guarantee on privacy and security, thus calling for a fundamental re-design.

SPEAKER BIOSKETCH

My T. Thai is a University of Florida (UF) Research Foundation Professor, Associate Director of UF Nelms Institute for the Connected World, and a fellow of IEEE. Dr. Thai's current research interests include Trustworthy AI, Blockchain, and Optimization. The results of her work have led to 7 books and 300+ publications in highly ranked international journals and conferences, including several best paper awards from the IEEE, ACM, and AAAI. The latest ones are AAAI 2023 Distinguished Papers Award and 2023 Web Science Trust Test-of-Time Award.

Dr. Thai received many recognitions, including UF Research Foundation professorship, IoT Term Endowed professorship, NSF CAREER Award, and DTRA Young Investigator Award. Among many professional activities, Dr. Thai currently serves as Editor-in-Chief of the Journal of Combinatorial Optimization, EiC of the IET Blockchain journal, and book series editor of Springer Optimization and Its Applications.